IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. No. 1:12-MD-2358 (SLR)
This Document Relates to: **All Actions**	

OPENING BRIEF IN SUPPORT OF DEFENDANT VIBRANT MEDIA INC.'S MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

OF COUNSEL

Edward P. Boyle
David N. Cinotti
Joeann E. Walker
Venable LLP
Rockefeller Center
1270 Avenue of the Americas
New York, NY 10020
(212) 307-5500
epboyle@venable.com
dncinotti@venable.com
jewalker@venable.com

Kelly E. Farnan (#4395)
Rudolf Koch (#4947)
Travis S. Hunter (#5350)
Richards, Layton & Finger
One Rodney Square
920 North King Street
Wilmington, DE 19801
(302) 651-7500
koch@rlf.com
farnan@rlf.com
hunter@rlf.com

DATED: May 1, 2013

Attorneys for Defendant Vibrant Media Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

RULES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

Pursuant to Federal Rule of Civil Procedure 12(b)(6), defendant Vibrant Media Inc. ("Vibrant") respectfully submits this opening brief in support of its motion to dismiss the Consolidated Class Action Complaint filed on December 19, 2012 (the "CAC") for failure to state a claim.

PRELIMINARY STATEMENT

Plaintiffs in this multidistrict litigation join a long line of claimants seeking windfall class-action damages for the placement on their computers of cookies—which are both benign and necessary for the Internet to function—without alleging that they suffered any legally cognizable harm. Similar cookie-related claims have been filed throughout the country and repeatedly dismissed at the outset of the case. Plaintiffs should fare no better than their unsuccessful predecessors.

None of the statutes that Plaintiffs invoke—the Stored Communications Act ("SCA"), the Computer Fraud and Abuse Act ("CFAA"), and the Electronic Communications Privacy Act (otherwise known as the "Wiretap Act")—reaches the conduct alleged in this case:

- First, Plaintiffs do not plead, and cannot plead, that Vibrant intentionally accessed a facility of an electronic communication service (i.e., a third-party company that provides email or Internet service) to access communications while in "storage," as required under the SCA. *See infra* Section I.
- Second, Plaintiffs do not allege that Vibrant caused them any damage or loss under the CFAA as defined in the statute, and certainly not $5,000 in loss to a single computer. *See infra* Section II.
- Third, Plaintiffs cannot establish that Vibrant, among other things, intercepted the contents of an electronic communication to which it was not a party, as required to violate the Wiretap Act. *See infra* Section III.

Accordingly, these claims should all be dismissed.

Although the alleged conduct and technology of each Defendant differs in many ways, the claims under the SCA, CFAA, and Wiretap Act fail against all Defendants for the same

reasons. In the interest of efficiency, Vibrant respectfully incorporates and adopts the arguments made by the other Defendants on their motions to dismiss, in addition to those arguments made in this opening brief.

FACTUAL BACKGROUND & NATURE AND STAGE OF PROCEEDINGS

Because the Court has pending before it four separate motions to dismiss the claims in the CAC and is undoubtedly familiar with the allegations and issues in the case, Vibrant will only briefly state the facts relevant to its motion and to Vibrant itself.

Vibrant is a provider of contextual advertising on the Internet. *See* CAC ¶¶ 16, 24. The CAC alleges that Plaintiffs browsed the Internet using non-party Apple Inc.'s Safari browser software and visited websites containing advertisements placed by Vibrant and the other Defendants. *Id.* ¶¶ 10-12. The CAC does not allege when Plaintiffs visited these websites. Nor does the CAC identify any particular advertisements that led to the placement of a cookie on any Plaintiff's computer.

Plaintiffs allege that their Safari browser settings were set by default to block third-parties, including advertising companies like Vibrant, from placing cookies on their computers. *Id.* ¶ 199. Cookies are a benign and beneficial part of the Internet environment. As one district court has explained, "[c]ookies *enable much of the information exchange that occurs on the Internet* by allowing the interactions between a specific computer and a web server to develop a memory of the communications between the two parties." *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001) (emphasis added). Websites use cookies to create a memory of necessary information like a registered user's login. *Id.* Cookies are not like listening devices that can be accessed and transmit information to whomever happens to be on the other side. Instead, "[a]ny cookie that is placed on a computer can only be read by the web

site that created it or an affiliated site." *Id.*; *see also* CAC ¶ 45.

Plaintiffs allege that a computer code was embedded in the advertisements delivered by Vibrant. *Id.* ¶ 146. After visiting a website containing the embedded code in those advertisements, Plaintiffs' browsers sent an invisible "form" to Vibrant. *Id.* According to Plaintiffs, Vibrant's response to the alleged transmitted form resulted in the placement or writing of a cookie to the user's computer. *Id.* ¶ 147. These cookies were allegedly "persistent," meaning that they did not expire after the user completed his or her browsing session. *See id.* ¶ 39.

Plaintiffs allege that when Plaintiffs visited a website, their browsers transmitted certain information—including the type of browser and operating system, the website address, an IP address, and screen resolution—to the website and the third-party advertising company that delivers advertisements to the webpage so that the webpage and the advertisements could be properly delivered and displayed. *See id.* ¶¶ 30-36, 41, 46. When a user visited a website that included an advertisement delivered by the advertising company that placed the cookie, the cookie transmitted an anonymous alphanumeric value assigned to that cookie, which the advertising companies allegedly used to associate information independently transmitted by the user's browser. *See id.* ¶¶ 45-46.

Although Plaintiffs devote much space in the CAC to the value of "personally identifiable information," Plaintiffs make only conclusory and unsupported allegations that the cookies at issue collected or transmitted such information, and the facts discussed above demonstrate that no such information was collected or transmitted.[1] Plaintiffs provide a partial quote from a *Wall Street Journal* article to further these assertions. Plaintiffs allege that a

[1] Conclusory allegations like these are "not entitled to be assumed true." *Ashcroft v. Iqbal*, 556 U.S. 662, 681 (2009).

Vibrant spokesman told the *Wall Street Journal* that Vibrant used the cookies "for unique user identification." *Id.* ¶ 151. But the full quote from the article is: "Vibrant . . . uses the technique for 'unique user identification,' the [Vibrant] spokesman said, *but doesn't collect personally identifiable information such as name or financial-account numbers*." Julia Angwin and Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, The Wall Street Journal (Feb. 17, 2012), http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html, Ex. A to Declaration of Edward P. Boyle ("Boyle Decl.") (emphasis added).[2]

Based on these allegations, the CAC asserts claims against Vibrant under: (1) the SCA, 18 U.S.C. § 2701 *et seq.*; (2) the CFAA, 18 U.S.C. § 1030; and (3) the Wiretap Act, 18 U.S.C. § 2510 *et seq.*

SUMMARY OF THE ARGUMENT

The CAC does not state any claims against Vibrant. First, Plaintiffs cannot base a claim under the SCA for Vibrant's alleged access to cookies located on Plaintiffs' computers. The SCA—which prevents hacking into facilities of electronic communication services like Internet service providers—does not apply here. The cookies and files on Plaintiffs' computers are not "facilities" of an "electronic communication service," and Vibrant did not allegedly access any communications while in storage, as required under the SCA.

Second, Plaintiffs do not state a claim under the CFAA. To maintain a cause of action under the statute, Plaintiffs must allege damage or loss as those terms are defined in the CFAA.

---

[2] The Court can consider the contents of the article on a motion to dismiss for failure to state a claim because it is cited in the CAC and relied on by Plaintiffs. *See Pension Benefit Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993).

They must also allege aggregate losses of at least $5,000 to the same computer. The CAC fails to do so.

Finally, for the reasons articulated by the other Defendants in their motions to dismiss, Plaintiffs' Wiretap Act claim also should be dismissed.

ARGUMENT

I. PLAINTIFFS HAVE NOT STATED A CLAIM UNDER THE SCA.

The SCA makes it an offense to "intentionally access[] without authorization a facility through which an electronic communication service is provided" and "thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The statute does not apply here because: (A) there is no allegation that Vibrant accessed a "facility through which an electronic communication service is provided," and (B) the communications at issue were not in "storage" in an electronic communication system.

A. Plaintiffs Have Not Alleged Access to a "Facility" Through Which Electronic Communication Services Are Provided

Plaintiffs' allegations that the Safari browser is a provider of electronic communication service and that files stored on Plaintiffs' computers called "browser-managed files" are facilities under the SCA, *see* CAC ¶¶ 216-17, are belied by the statute's plain language.

The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Courts have recognized that telephone companies, Internet or e-mail service providers, and bulletin board services provide electronic communication services. *See Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 792 (5th Cir. 2012), *petition for cert. filed*, (U.S. Apr. 16, 2013) (No. 12-1264). In other words, "electronic communication services" are, like America

Online, Yahoo!, and Hotmail, third-party entities that provide a service that enables users or subscribers with accounts with the service provider to send or receive electronic communications. *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008), *rev'd on other grounds sub nom. City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010) (holding that wireless company provided electronic communication services because it "provided a 'service' that enabled [the parties] to 'send or receive . . . electronic communications,' i.e., text messages"); *see also Garcia*, 702 F.3d at 793 ("'[T]he statute envisions a provider (the ISP or other network service provider) and a user (the individual with an account with the provider), with the user's communications in the possession of the provider.'" (quoting Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215 n.47 (2004))); S. Rep. No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568, 1986 WL 31929, at *14 ("Existing telephone companies and electronic mail companies are providers of electronic communication services. Other services like remote computing services may also provide electronic communication services.").

Thus, while companies that provide email or Internet services are providers of electronic communication services, software applications like the Safari browser are not electronic communication services or providers of such services. In ordinary English usage, no one would refer to a browser as a "service," or call a software application like Safari a "provider" of a service. Congress is presumed to use the ordinary meaning of words. *See Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252 (2004).

Files stored on Plaintiffs' computer are also not "facilities" through which an electronic communication service is provided. Courts have recognized that "the relevant 'facilities' that the SCA is designed to protect are not computers that *enable* the use of an electronic communication

service, but instead are facilities that are *operated by* electronic communication service providers and used to store and maintain electronic storage." *Garcia*, 702 F.3d at 792 (quoting *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 2:11–cv–01073, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012)). And courts have correctly rejected the view that home computers and files contained on them are "facilities" through which electronic communication services are provided. *See, e.g.*, *id.* at 793; *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1068 (N.D. Cal. 2012) ("*iPhone II*"); *Freedom Banc*, 2012 WL 3862209, at *9; *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001); *see also* Computer Crime & Intellectual Property Section, Criminal Division, U.S. DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 126 (1999) (stating that the SCA does not apply to emails "not stored on the server of a third-party provider of RCS [remote computing services] or ECS [electronic communication services]"), *available at* http://www.justice.gov/criminal/ cybercrime/ docs/ssmanual2009.pdf.

Moreover, Plaintiffs' interpretation of the terms "facility" and "electronic communication service" to mean the contents of their hard drives and their Safari browser would lead to absurd results. *See In re Kaiser Aluminum Corp.*, 456 F.3d 328, 338 (3d Cir. 2006) ("A basic tenet of statutory construction is that courts should interpret a law to avoid absurd or bizarre results."). The SCA exempts from its scope conduct authorized by "*the person or entity providing* a wire or electronic communications service." 18 U.S.C. § 2701(c)(1) (emphasis added). It would be nonsensical to describe the Safari software as a "person" or "entity," or ask whether Safari has authorized the conduct at issue in the case. In addition, if Safari were a provider of electronic communications services, then, under the plain language of the statute, Safari would have the authority to permit access to Plaintiffs' computer files as facilities of those services. *See*

Crowley, 166 F. Supp. 2d at 1271 (rejecting argument that plaintiff's computer was a facility under the SCA because "[i]t would certainly seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of [plaintiff's] argument").

The SCA also prohibits an electronic communication service from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," unless an exception applies. *See* 18 U.S.C. § 2702(a)(1), (b)-(c) . A computer program like Safari cannot "knowingly" do anything. The statute further provides that it shall not be unlawful for "an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment." *Id* § 2511(2)(a)(i). Safari has no officers, employees or agents who could interpret, disclose, or use any communications.

These are just a few examples of the disconnect between Plaintiffs' purported statutory construction and the statute itself.

B. Plaintiffs Have Not Alleged That the Communications at Issue Were in Electronic Storage.

Plaintiffs' SCA claim also fails because the communications that Vibrant allegedly accessed were not in electronic storage. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17). The "communications" allegedly accessed were not in electronic storage under this definition.

"[I]nformation that an Internet provider stores to its servers or information stored with a telephone company—if such information is stored temporarily pending delivery or for purposes of backup protection—are examples of protected electronic storage under the statute." *Garcia*, 702 F.3d at 793. Plaintiffs' allegations are nowhere near this paradigm. Plaintiffs allege that cookies placed on their computers communicated an alphanumeric value that allowed Vibrant to associate with that value other information sent independently by Plaintiffs' browsers. *See, e.g.*, CAC ¶¶ 46, 217. Any such "communications" were not temporarily stored pending delivery to a recipient, unlike temporary storage by an Internet service provider pending delivery of an email communication. *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512-13 (S.D.N.Y. 2001) (holding that communications from cookies on plaintiffs' computers were not in electronic storage under the SCA because they were not stored "'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it"). Courts have held that emails and other communications stored on a user's computer or phone are not in temporary, intermediate storage incidental to their transmission. *See, e.g.*, *Garcia*, 702 F.3d at 793; *Freedom Banc*, 2012 WL 3862209, at *9.

In addition, Plaintiffs claim that the cookies allegedly placed by Vibrant on their computers were persistent, not temporary. *See, e.g.*, CAC ¶ 39(a)(ii) (alleging that a "persistent cookie" can "stay on a user's device for years" and be used to "track users' actions on the Internet"). Information transmitted from a persistent cookie is not in temporary storage. *See In re Toys R Us Inc. Privacy Litig.*, No. 00-CV-2746, 2001 WL 34517252, at *3 (N.D. Cal. Oct. 9, 2001) (relying on allegation that cookies at issue remained on plaintiffs' computers indefinitely

to hold that information obtained from cookies was not in temporary storage); *In re DoubleClick*, 154 F. Supp. 2d at 512 (same).

The "communications" at issue were also not stored "by an electronic communication service for purposes of backup protection." The CAC contains no allegations that any information on Plaintiffs' computers was saved there for purposes of backup protection, and, as explained above, Plaintiffs' Safari browser is not an electronic communication service. *See supra* Section I.A.

Finally, in an attempt to plead a claim under the Wiretap Act, Plaintiffs allege that Defendants "intercepted Class Members electronic devices contemporaneously with the transmission of those communications." CAC ¶ 208. That allegation is fatal to their claim that the communications were in electronic storage under the SCA because "messages in electronic storage cannot, by definition, be acquired contemporaneously." *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998).

II. PLAINTIFFS HAVE NOT STATED A CLAIM UNDER THE CFAA.

To state a claim under the CFAA, Plaintiffs must allege both a violation of one of the substantive prohibitions in 18 U.S.C. § 1030(a) and meet the requirements of 18 U.S.C. § 1030(g). As set forth below, the CAC fails to plead the necessary requirements of Section 1030(g) to maintain a civil cause of action.

Section 1030(g) provides:

> Any person who suffers *damage or loss* by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought *only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).* Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are *limited to economic damages.*

18 U.S.C. § 1030(g) (emphasis added). The factors set forth in subsection (c)(4)(A)(i)(I)-(V) of the statute are: (I) "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value"; (II) modification or impairment of medical examinations, diagnosis, or treatment; (III) physical injury; (IV) a threat to public health or safety; and (V) damage to a computer used by the United States Government for the administration of justice, national defense, or national security. *Id.* § 1030(c)(4)(A)(i)(I)-(V) . Based on the allegations of the CAC, the only possible statutory factor at issue here is subsection (A)(i)(I)—loss of at least $5,000 in value.

Because the CAC fails to allege that Plaintiffs have suffered economic damage or loss in an amount during any one-year period aggregating at least $5,000 in value, the CFAA claim should be dismissed.

A. The CAC Fails to Allege that Plaintiffs Suffered "Damage or Loss" As Defined in the CFAA.

The CAC fails to adequately plead that Plaintiffs have suffered any damage or loss within the meaning of the statute. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). Damage or loss must be economic. *Id.* § 1030(g).

Plaintiffs do not allege any impairment to the integrity or availability of their data, programs, computer systems, or information, and therefore do not allege economic damage. Plaintiffs do not claim that they lost any of their information or data through Vibrant's alleged placement or use of cookies. And the alleged placement of cookies on Plaintiffs' computers did not cause any damage to Plaintiffs' computers or software.

The CAC also does not allege loss within the meaning of the CFAA. Plaintiffs seek to plead economic loss based entirely on the purported "monetary and trade value" of the information that Vibrant allegedly collected. *See, e.g.*, CAC ¶ 49. Even if the information allegedly obtained had any economic value, the transmission or collection of such information is not "loss" under the statute. The economic loss alleged must be a "reasonable cost" to Plaintiffs relating to investigating or fixing damage caused by a violation of the statute, such as restoring data, programs, systems or information to their condition prior to the alleged offense; or consequential damages as a result of "interruption of service." *See* 18 U.S.C. § 1030(e)(11); *see also Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, No. 09–2751, 2011 WL 6088611, at *4–5 (E.D. Pa. Dec. 7, 2011) ("A compensable 'loss' under the CFAA . . . is a loss which is in some way related to functionality of the protected computer at issue. Either the loss is the cost of remedial measures taken to investigate or repair the damage to the computer, or the loss is the amount of lost revenue resulting from a plaintiff's inability to utilize the computer while it was inoperable because of a defendant's misfeasance."); *M-I LLC v. Stelly*, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010) ("[C]ase law has consistently interpreted the loss provision to encompass only the costs incurred as a result of investigating or remedying damage to a computer, or costs incurred because the computer's service was interrupted.").

Here, Plaintiffs do not allege that their computer services were interrupted as a result of any alleged conduct by Vibrant. Nor do Plaintiffs allege facts indicating that they incurred any costs relating to investigating or remedying computer damage. They have thus failed to plead any cognizable loss under the CFAA.

Plaintiffs may not base a CFAA claim merely upon the allegation that Vibrant collected any information without authorization. Such a claim does not fit within the plain language of the statute, and case law has established that the allegedly unauthorized collection or use of a plaintiff's information, without accompanying damage to the plaintiff's computer or system, is not a "loss" under the statute. *See, e.g.*, *Yunker v. Pandora Music, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (holding that alleged transfer of personal information to advertisers was not "loss" under the CFAA); *iPhone II*, 844 F. Supp. 2d at 1068 ("[C]ourts have tended to reject the contention that personal information . . . constitutes economic damages under the CFAA"); *Del Vecchio v. Amazon.com, Inc.*, No. 11-366, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) ("It is not enough to allege only that the [plaintiffs'] information has value to Defendant; the term 'loss' requires that Plaintiffs suffer a detriment—a detriment amounting to more than $5,000."); *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448, at *8 (E.D. Pa. Dec. 22, 2011) ("Claims of lost business opportunities, damaged reputation, loss of assets, and other missed revenue . . . do not constitute [CFAA] 'loss.'"); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 614-15 (M.D. Tenn. 2010) (holding that misappropriation of confidential information is not a "loss" under the CFAA).

B. Plaintiffs Have Not Alleged At Least $5,000 in Loss Within a One-year Period.

Yet another reason to dismiss the CFAA claim is that Plaintiffs have not sufficiently alleged "loss to 1 or more persons during any 1-year period (and, for purposes of an

investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value," under 18 U.S.C. § 1030(c)(4)(A)(i)(I), as incorporated in Section 1030(g).

1. The CAC's Conclusory Allegations Do Not Sufficiently Plead $5,000 in Loss.

As explained above, the alleged collection of information through cookies does not qualify as a "loss" under the CFAA. Moreover, even if the CFAA permitted Plaintiffs to proceed under such a theory, the CAC does not allege any facts to show that Plaintiffs suffered losses "during a one-year period aggregating at least $5,000 in value." CAC ¶¶ 225-27. The CAC does not quantify the economic losses specific to any Plaintiff or provide the dates on which Vibrant allegedly collected information from any Plaintiff to establish that the losses occurred within a one-year period. The Court should not give any weight to Plaintiffs' conclusory assertions, in the absence of supporting allegations of fact. *See Iqbal*, 556 U.S. at 681.[3]

The CAC's allegations regarding a survey of Internet users are not sufficient to meet the CFAA's $5,000 threshold. These allegations state merely that the organizers of a survey involving 180 Internet users concluded that web browsing history could be valued at $52 per year. CAC ¶ 56. There is no allegation that this $52 figure represents any loss within the meaning of the CFAA. *See Del Vecchio*, 2012 WL 1997697, at *4. Nor is it even clear that the

---

[3] In their opposition to Google Inc.'s motion to dismiss the CAC, Plaintiffs rely on *Oracle America, Inc. v. Service Key, LLC*, No. C 12-00790 SBA, 2012 WL 6019580 (N.D. Cal. Dec. 3, 2012), to argue that they need not allege $5,000 in loss. *See* Plfs.' Opp. to Google Mot. to Dismiss, ECF No. 81, at 25. *Oracle* is inapposite because it addresses a different $5,000 statutory requirement than the one at issue here. *See Oracle*, 2012 WL 6019580, at *4 (addressing the $5,000 requirement in 18 U.S.C. § 1030(a)(4), not § 1030(c)(4)(A)(i)(I)). Section 1030(a)(4), which was at issue in *Oracle*, provides that a defendant violates the CFAA if it accesses a protected computer and obtains anything of value; if the only thing of value is the use of the computer, the value of the use must be at least $5,000. The $5,000 threshold here, in contrast, is required for Plaintiffs to maintain a civil cause of action under Section 1030(g).

alleged survey concerned the same kind of data that was allegedly collected from Plaintiffs in this action. And finally, the alleged $52 value of this information to each Plaintiff falls well short of the $5,000 statutory threshold.

2. The Plaintiffs Can Not Add Up Purported Losses By All Plaintiffs and Class Members to Reach $5,000.

Plaintiffs cannot satisfy the CFAA's $5,000 statutory threshold by aggregating alleged losses to different computers used by different members of the putative class at different times. Interpretation of the aggregation provision in the statute must, of course, begin with the statutory text. *See BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004). As part of that textual analysis, the Court must read statutory phrases together, not in isolation. *See Samantar v. Yousuf*, 130 S. Ct. 2278, 2289 (2010).

Applying those principles here, the unambiguous statutory language does not permit Plaintiffs to add up the purported losses to different computers (even if there were any cognizable losses) used by the various putative class members affected by a defendant's alleged course of conduct. The statute provides that losses "resulting from a related course of conduct affecting 1 or more other protected computers" may *only* be aggregated "for purposes of an investigation, prosecution, or other proceeding brought by the United States." 18 U.S.C. § 1030(c)(4)(A)(i)(I). Since aggregation of losses from multiple computers based on a related course of conduct is "only" permitted for government investigations or prosecutions, it is obviously not permitted for a private civil action like this one. *See Lyons v. Coxcom, Inc.*, No. 08-CV-02047-H, 2009 WL 347285, at *8 (S.D. Cal. Feb. 6, 2009) ("[U]nder the language of the statute, only federal prosecutors may aggregate losses across multiple protected computers from a related course of conduct."), *vacated on other* grounds, 718 F. Supp. 2d 1232 (S.D. Cal. 2009; *see also Shell Oil Co. v. Manley Oil Corp.*, 124 F.2d 714, 715 (7th Cir. 1941) (holding that the

word "only" was unambiguously a "limiting and restrictive term which qualifies" the words surrounding it and meant "nothing else" but what it limits).

Legislative history confirms this interpretation. At the request of the government, Congress added the relevant language to what was then 18 U.S.C. § 1030(a)(5) as part of the 2001 USA PATRIOT Act. *See* Pub. L. No. 107-56, § 814(a), 115 Stat. 272 (2001) (adding language under heading "Clarification of Protection of Protected Computers"). *Compare* 18 U.S.C. § 1030(a)(5) (2001) (attached as Ex. B to Boyle Decl.) *with* 18 U.S.C. § 1030(a)(5) (2002) (attached as Ex. C to Boyle Decl.). A year prior to the addition of this clause to the statute, Attorney General Janet Reno testified before a House subcommittee:

> [W]e may need to strengthen the Computer Fraud and Abuse Act by *closing a loophole that allows computer hackers who have caused a large amount of damage to a network of computers to escape punishment if no individual computer sustained over $5,000 worth of damage.*

Hearing Before the Subcomm. on Commerce, Justice, State and Judiciary of the Senate Comm. on Appropriations, 106th Cong. (Feb. 16, 2000), 2000 WL 177323 (emphasis added).

In 2001, Congress closed the "loophole" that Attorney General Reno discussed for government investigation and prosecutions, but rejected a broader proposal that would have applied the new provision to private civil actions as well. *See* 18 U.S.C. 1030(a)(5)(B)(i) (2002) (prohibiting acts that cause "loss to 1 or more persons during any 1-year period (*and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only*, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value" (emphasis added)). In October 2000, the House Judiciary Committee proposed an amendment that would have prohibited conduct that "caused loss to one or more persons during any one-year period (including loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000." H.R.

Rep. No. 106-932 (2000), 2000 WL 1474589, at *4. This amendment did not limit aggregation for losses affecting multiple computers to government prosecutions and investigations. The House Report accompanying the bill explains that the proposed amendment "clarifies that damage to multiple protected computers must be aggregated in determining whether a violation has exceeded the $5,000 threshold for a Federal offense." *Id.* at *20. That same language was also included in the Senate's version of the bill, *see* 147 Cong. Rec. S10717-01, § 815, 2001 WL 1220966, but ultimately was not adopted by Congress.

Congress's rejection of the broader proposed amendment is strong evidence that it intended to limit aggregation of losses to multiple computers to government prosecutions and investigations. *See William A. Graham Co. v. Haughey*, 568 F.3d 425, 436 (3d Cir. 2009) (relying on Congress's consideration and rejection of particular language to interpret statute). Therefore, in a private civil action under the CFAA any losses to be aggregated must be to the same computer. *See, e.g.*, *Thurmond v. Compaq Computer Corp.*, 171 F. Supp. 2d 667, 680-81 (E.D. Tex. 2001) (holding that CFAA prior to 2001 amendment required $5,000 in loss be to a single computer and citing Attorney General's testimony in support of that interpretation).

Some district courts have overlooked the CFAA's plain language. These courts have instead relied upon a Senate Report accompanying the 1986 original version of the CFAA to interpret the aggregation provision, and have held that the CFAA permits aggregation if the losses were attributable to the "same act." *See, e.g.*, *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *11 (N.D. Cal. Sept. 20, 2011); *In re DoubleClick*, 154 F. Supp. 2d at 522; *see also* S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482-83, 1986 WL 31918, at *5. As explained above, the relevant legislative history on this issue is that surrounding the 2001 amendment to the CFAA. If the original statute permitted

aggregation of losses to multiple computers, there would have been no need for the 2001 amendment that the Attorney General requested.

But even using the 1986 Senate Report as a guide to the statute's meaning, Plaintiffs have not stated a claim. The Senate Report states that "[b]y using 'one or more others', the [Senate Judiciary] Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the [then] $1,000 threshold." S. Rep. No. 99-432, 1986 U.S.C.C.A.N. at 2482-83, 1986 WL 31918, at *5. The Judiciary Committee was concerned about hacking into a computer that caused losses to multiple individuals, though not $1,000 in loss to any one individual.[4] In the Report, the Committee used the example of an incident at Memorial Sloan-Kettering Cancer Center, in which hackers gained access to the treatment records of 6,000 patients. *Id.* at 2480, 1986 WL 31918, at *2-3. In that case, the "same act" affected more than one individual and would be covered by the statute if the losses to those individuals aggregated at least $1,000 (or $5,000 under the current version of the statute).

In contrast, the alleged conduct of writing cookies to the computers of different putative class members after they visited diverse (and unspecified) websites containing diverse (and unspecified) advertisements on diverse (and unspecified) dates cannot reasonably be considered part of the "same act." *See, e.g.*, *Chance*, 165 F. Supp. 2d at 1159 ("It is undisputed that each time a web page sends a message to a user's computer instructing the computer to communicate the contents of the cookie on the user's hard drive with Avenue A, it is an individual, singular act."). To the extent that there is ambiguity in the statute as to whether Plaintiffs may aggregate purported losses across an uncertified putative class using different computers, the rule of lenity

[4] The statute at the time it was passed criminalized conduct that caused "loss to one or more others of a value aggregating $1,000 or more during any one year period." 18 U.S.C. § 1030(a)(5)(A) (1982 & Supp. V, 1983-1988) (attached as Ex. D to Boyle Decl.).

requires an interpretation in favor of Defendants here. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (holding that the rule of lenity applies where the court is applying an ambiguous criminal statute invoked in a civil action); *Crandon v. United States*, 494 U.S. 152, 168 (1990) (same).

III. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE WIRETAP ACT.

For the reasons discussed in the other Defendants' motions, Plaintiffs have failed to state a claim under the Wiretap Act. *See* Def. Google Inc.'s Opening Br. in Supp. of Mot. to Dismiss the CAC, ECF No. 57, at 16-19; Mem. of Law in Supp. of Def. Pointroll, Inc.'s Mot. to Dismiss, ECF No. 53, at 11-15; Reply Br. in Supp. of Def. Pointroll, Inc's Mot. to Dismiss, ECF No. 89, at 4-7; Def. Google Inc.'s Reply Br. in Supp. of Mot. to Dismiss the CAC, ECF No. 90, at 5-8; Mem. of Law in Supp. of Mot. to Dismiss of Defs. Media Innovation Grp. LLC & WPP PLC.

Vibrant adopts and incorporates those arguments here.

CONCLUSION

For the reasons set forth above, Vibrant respectfully requests that the Court dismiss the CAC with prejudice pursuant to Federal Rule of Civil Procedure 12(b)(6).

OF COUNSEL:
Edward P. Boyle
David N. Cinotti
Joeann E. Walker
Venable LLP
Rockefeller Center
1270 Avenue of the Americas
New York, NY 10020
(212) 307-5500
epboyle@venable.com
dncinotti@venable.com
jewalker@venable.com

Dated: May 1, 2013

/s/ Rudolf Koch

Kelly E. Farnan (#4395)
Rudolf Koch (#4947)
Travis S. Hunter (#5350)
Richards, Layton & Finger
One Rodney Square
920 North King Street
Wilmington, DE 19801
(302) 651-7500
koch@rlf.com
farnan@rlf.com
hunter@rlf.com

Attorneys for Defendant Vibrant Media Inc.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of Court for the United States District Court for the District of Delaware by using the CM/ECF system. I certify that for all participants in the case that are registered CM/ECF users, service will be accomplished via the CM/ECF system.

/s/ Rudolf Koch
Rudolf Koch (#4947)